Vulnerability Alert

Alert No : AVA171013

Date : 16-Oct-17 16:31 PM

Taiwan Bank Heist: Malware Information

Overview

New information has been revealed on the malware that was used by the attackers in the Taiwan Bank heist.

Description / Impact

FINCSIRT have received information from several sources on the malware that was used in the Taiwan Bank heist (reported by FINCSIRT using AIA171009). Please use the following information to empower your perimeter security measures to prevent same attack. FINCSIRT will be sharing more information, as soon as we receive.

The list of the malware used,

File Name	Signature	SHA1
msmpeng.exe	BKDR_KLIPOD.ZTEJ-A	bdb632b27ddb200693c1b0b80819a7463d4e7a98
splwow32.exe	BKDR_KLIPOD.ZTEJ-B	c7e7dd96fefca77bb1097aeeefef126d597126bd
FileTokenBroker.dll	TROJ_BINLODR.ZTEJ-A	f891fde8908ae18801d7a0be1eeab07391c00c1b
bitsran.exe	RANSOM_HERMS.A	b30daf74b25b8615ada10cca195270c32e6b343a
RSW72CE.tmp	RANSOM_HERMS.A	d08573c5e825b7beeb9629d03e0f8ff3cb7d1716

The list of the Command and Control (C&C) Servers

- 94.23.148.41
- 167.114.32.112

Risk Reduction Recommendations

Immediate Actions to be taken:

1. Use the above give information to configure to detect/restrict any communication regarding your infrastructure.
2. This is only an additional step in defending your infrastructure and you should always follow the original recommendations given by the AIA171009.
3. It is highly advisable to inform the staff to be vigilant.
4. Inform FINCSIRT on any findings or incidents as soon as it is occurred.

Reference

https://www.ithome.com.tw/news/117401

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Financial Sector Computer Security Incident Response Team, Sri Lanka
Hotline: + 94 112039777
Report incident to incident@fincsirt.lk